UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

ATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
0931,004	08/17/2001	Nang Kon Kwan	06502.0336	2756

7590 03/18/2005

Finnegan, Henderson, Farabow,
Garrett & Dunner, L.L.P.
1300 I Street, N.W.
Washington, DC 20005-3315

EXAMINER	
CHAI, LONGBIT	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 03/18/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/931,004	KWAN, NANG KON	
	Examiner	Art Unit	
	Longbit Chai	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 January 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☐ Claim(s) _____ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-33* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *21 October 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Priority

1. No claim for priority has been made in this application.

The effective filing date for the subject matter defined in the pending claims in this application is 8/17/2001.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1 – 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bisbee (Patent Number: 6367013), in view of CFSB ("How Key Escrow Might Work", by Computer Fraud & Security Bulletin, July 1, 1996).

As per claim 1, 15, 19 and 33, Bisbee teaches method in a data processing system for requesting a digital certificate from a certificate authority and archiving an encryption key outside of the certificate authority, comprising:

receiving a request from a user for a digital certificate (Bisbee: see for example, Column 11 Line 64 – 66 and Column 12 Line 28 – 30: RA (Registration Manager) as taught by Bisbee is responsible to request a digital certificate between the subscriber and CA (Certificate Authority)).

Bisbee teaches TCU (Trusted Custodial Utility) is a trusted 3rd-party repository of information objects and securely stores and securely retrieves digitally signed, authenticated and encrypted information objects and provides for backup and disaster recovery (Bisbee: see for example, Column 3 Line 38 – 39, Column 3 Line 55 – 57 and Column 3 Line 62 – 63).

Bisbee does not disclose expressly receiving an indication of proof of archival of the user's encryption key associated with the request.

CFSB teaches receiving an indication of proof of archival of the user's encryption key associated with the request (CFSB: see for example, 1st Paragraph: CFSB teaches with an escrowed infrastructure, a user's private encryption key would be archived with a trusted key holder prior to issuance of he corresponding public key certificate; and for the case of 3rd-party trusted key holder, the CA needs proof of that key has been escrowed (i.e. archived), say, through the escrow certificate digitally signed by the key holder).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of CFSB within the system of Bisbee because CFSB teaches providing benefits to owners for archiving key especially for the

situation even after acquiring the new key pair, data retransmission is not possible (e.g. voice mailbox messages) (CFSB: see for example, page 2, 5th Paragraph).

Accordingly, Bisbee in view of CFSB teaches receiving an indication of proof of archival of the user's encryption key associated with the request, wherein the user's encryption key is archived under control of an entity other than the certificate authority.

As per claim 18, Bisbee teaches a data processing system for requesting a digital certificate from a certificate authority and archiving an encryption key under control of an entity other than the certificate authority, comprising:

a registration manager configured to receive a digital certificate request including a user's encryption key (Bisbee: see for example, Column 11 Line 52 – 66: the public key is used as the basis for a certificate request, where the basis is uniquely associated with a key-pair assigned to a reference handle (or name)).

Bisbee does not disclose expressly sending the user's encryption key, and in response receive an indication of proof of archival.

CFSB teaches receiving an indication of proof of archival of the user's encryption key associated with the request (CFSB: see for example, 1st Paragraph: CFSB teaches with an escrowed infrastructure, a user's private encryption key would be archived with a trusted key holder prior to issuance of he corresponding public key certificate; and for the case of 3rd-party trusted key holder, the CA needs proof of that key has been escrowed (i.e. archived), say, through the escrow certificate digitally signed by the key holder).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of CFSB within the system of Bisbee because CFSB teaches providing benefits to owners for archiving key especially for the situation even after acquiring the new key pair, data retransmission is not possible (e.g. voice mailbox messages) (CFSB: see for example, page 2, 5th Paragraph).

Accordingly, Bisbee in view of CFSB teaches a registration manager configured to receive a digital certificate request including a user's encryption key, send the user's encryption key, and in response receive an indication of proof of archival.

a certificate authority configured to issue a digital certificate when it is determined that an indication proof of archival was received (CFSB: see for example, 1st Paragraph).

Furthermore, Bisbee teaches TCU (Trusted Custodial Utility) is a trusted 3rd-party repository of information objects and securely stores and securely retrieves digitally signed, authenticated and encrypted information objects and access to the data repository (i.e. database) that provides for backup and disaster recovery (Bisbee: see for example, Column 3 Line 38 – 39, Column 3 Line 50 – 55, Column 3 Line 55 – 57 and Column 3 Line 62 – 63).

Accordingly, Bisbee in view of CFSB teaches a data recovery manager (i.e. equivalent toTCU as taught by Bisbee) configured to receive the user's encryption key, send the user's encryption key to a database controlled by an entity other than the certificate authority for archiving, create an indication of proof archival and send the indication of proof of archival.

a database, under control of an entity other than the certificate authority, configured to receive and archive the user's encryption key (Bisbee: see for example, Column 3 Line 50 – 52: the data repository is qualified as the database).

As per claim 2 and 20, Bisbee in view of CFSB teaches the claimed invention as described above (see claim 1 and 19 respectively). CFSB further teaches the step of sending a digital certificate associated with the user in response to the received request and indication of proof of archival (CFSB: see for example, 1st Paragraph).

As per claim 3 and 21, Bisbee in view of CFSB teaches the claimed invention as described above (see claim 1 and 19 respectively). Bisbee further teaches receiving the user's encryption key (Bisbee: see for example, Column 11 Line 52 – 66: the public key is used as the basis for a certificate request, where the basis is uniquely associated with a key-pair assigned to a reference handle (or name)).

As per claim 4 and 22, Bisbee in view of CFSB teaches the claimed invention as described above (see claim 3 and 21 respectively). Bisbee further teaches the encryption key is encrypted during transmission, and wherein the method further comprises the step of decrypting the encrypted encryption key (Bisbee: see for example, Column 11 Line 64 – 66 and Column 11 Line 52 – 60: (a) certificate request is signed by RA and thereby is encrypted (b) the public key is used as the basis for a

certificate request, where the basis is uniquely associated with a key-pair assigned to a reference handle (or name)).

As per claim 5 and 23, Bisbee in view of CFSB teaches the claimed invention as described above (see claim 3 and 21 respectively). CFSB further teaches the encryption key is the user's private key (CFSB: see for example, Page 1, 1st Paragraph, Line 1 – 4).

As per claim 6 and 24, Bisbee in view of CFSB teaches the claimed invention as described above (see claim 4 and 22 respectively). Bisbee further teaches a data recovery manager that receives and manages archiving of the encryption key, and wherein the encryption key is encrypted during transmission using the data recovery manager's public transport key (Bisbee: see for example, Column 13 Line 19 – 25).

As per claim 7, 11, 13, 25, 29 and 31, Bisbee in view of CFSB teaches the claimed invention as described above (see claim 1, 10, 12, 19, 28 and 30 respectively). CFSB teaches the indication of proof of archival is digitally signed, and wherein the method further comprises the step of verifying a digital signature on the indication of proof of archival Page 1, 1st Paragraph, Line 6 – 7).

As per claim 8 and 26, Bisbee in view of CFSB teaches the claimed invention as described above (see claim 7 and 25 respectively). Bisbee teaches the indication of

proof of archival is digitally signed by the data recovery manager (Bisbee: see for example, Column 13 Line 19 – 25).

As per claim 9, 14, 27 and 32, Bisbee in view of CFSB teaches the claimed invention as described above (see claim 1, 13, 19 and 31 respectively). Bisbee in view of CFSB teaches the user's encryption key is archived under control of the user (Bisbee: see for example, Column 11 Line 52 – 66: the public key is used as the basis for a certificate request, where the basis is uniquely associated with a key-pair (generated by the user's smart card) assigned to a reference handle (or name)).

As per claim 10, 16 and 28, Bisbee teaches a method in a data processing system for requesting a digital certificate from a certificate authority and archiving an encryption key outside of the certificate authority, comprising:

sending a request for a digital certificate (Bisbee: see for example, Column 11 Line 64 – 66 and Column 12 Line 28 – 30: RA (Registration Manager) as taught by Bisbee is responsible to request a digital certificate between the subscriber and CA (Certificate Authority)).

Bisbee teaches TCU (Trusted Custodial Utility) is a trusted 3rd-party repository of information objects and securely stores and securely retrieves digitally signed, authenticated and encrypted information objects and provides for backup and disaster recovery (Bisbee: see for example, Column 3 Line 38 – 39, Column 3 Line 55 – 57 and Column 3 Line 62 – 63).

Bisbee does not disclose expressly the request having an indication of proof of archival of an encryption key for the user.

CFSB teaches receiving an indication of proof of archival of the user's encryption key associated with the request (CFSB: see for example, 1st Paragraph: CFSB teaches with an escrowed infrastructure, a user's private encryption key would be archived with a trusted key holder prior to issuance of he corresponding public key certificate; and for the case of 3rd-party trusted key holder, the CA needs proof of that key has been escrowed (i.e. archived), say, through the escrow certificate digitally signed by the key holder).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of CFSB within the system of Bisbee because CFSB teaches providing benefits to owners for archiving key especially for the situation even after acquiring the new key pair, data retransmission is not possible (e.g. voice mailbox messages) (CFSB: see for example, page 2, 5th Paragraph).

receiving a digital certificate in response to the request (CFSB: see for example, page 1, 1st Paragraph, Line 2).

As per claim 12, 17 and 30, claims 12, 17 and 30 are similar to claim 1. Therefore, see rationale addressed above in rejecting claim 1.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Longbit Chai
Examiner
Art Unit 2131

LBC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100